Social Media, a New Challenge for Law Enforcement, Schools, and Youth

by

Captain Paul Bockrath
Fairfield Police Department

May 2011

COMMAND COLLEGE CLASS XXXXVIII

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

Social Media, a New Challenge for Law Enforcement, Schools, and Youth

The development and use of social media technology is evolving exponentially and so too is the exploitation of this medium for nefarious purposes. The proliferation of social media communication into mainstream society has provided a fertile medium for individuals to exploit this technology and its users in ways most law enforcement agencies are ill equipped or unprepared to investigate scrupulously. Law enforcement agencies have primarily relied on traditional investigative models and tactics to address crime and more recently cybercrime. Social networking sites and other forms of social media technology, though, offer an even greater challenge to law enforcement, schools and youth due to their evolution, rapid growth, accessibility, and allure.

The challenge is the various problems and concerns associated with the use of social media technology, and how law enforcement, schools and youth who use social media can collaborate to address the myriad of issues associated with its use. On the pages that follow, I will outline the most pressing concerns, explain why they are significant, and offer solutions to create a safer and more productive use of the virtual world within which it exists.

The Fundamental Shift

The blending of technology and social interaction has resulted in a fundamental shift in the way people communicate. With more than 500 million active users on Facebook alone, this new form of communication has changed not only the way people communicate with each other but also what personal information or access they allow to

others (Facebook, 2010). Social media can include any form of multi-media used to communicate or share information, data, images, video or other content interactively with one or multiple people simultaneously. Social media technology is the platform by which this communication is shared to include computers, gaming systems, GPS systems, smartphones, and tablet technologies.

The sophistication of this technology allows users to not only share content with a specific intended recipient, but with anyone in the world who chooses to access it. The rapid growth in social media technology is only matched by the profound growth in its users. According to a 2009 report on Adults and Social Networking Sites by the Pew Research Center, 35% of adult Internet users and 65% of teenaged Internet users have a profile on an online social networking site. For online adults 18- 24 years, 75% have a profile on an online social networking site (Lenhart, 2009). Facebook, the most popular peer-to-peer social networking site, has more than 500 million of the estimated billion social media users in 190 countries worldwide (Facebook, 2010). This explosive growth and sophistication of social media technology has created opportunities to exploit this technology with a virtually unrestricted, unmonitored and unregulated access from one user to another. Unfortunately, this also allows one to victimize others in ways and in numbers never before imagined.

Social media users, platforms, and sites have outpaced the ability of most law enforcement agencies to identify, investigate and prosecute the associated crimes and the victimization of individuals using these technologies. A May 2010 survey of mid-sized California law enforcement agencies showed that 63% did not have full time sworn personnel assigned to investigate social media or cybercrimes. Further, 33% did not even

have part-time sworn personnel assigned to investigate social media or cybercrimes. This staffing disparity is in spite of the same agencies reporting that 70% experienced a social media related crime in the last year (Bockrath, 2010).

Law enforcement has made tremendous strides to address white-collar cybercrimes such as fraud, identity theft, embezzlement and cybercrimes against children such as child pornography. Many other forms of victimization have emerged with the advent of social media, many of which have yet to be codified as a criminal offense. These acts include: cyberbullying, defamation or slanderous Internet postings, unauthorized posting of surreptitious video or images, sexting, intimidation, or the solicitation of violence upon another person, to include cyber-facilitated assaults on unsuspecting victims.

One of the most prevalent forms of victimization is cyberbullying, or "electronic aggression," identified in 2008 by the CDC as an "emerging public-health problem" (Billitteri, 2008). In a 2008 study by UCLA Psychology Professor Jaana Juvonen, 41% of teenagers surveyed reported being the victim of cyberbullying between one and three times over the course of a year (Wolpert, 2008). Bullying victims often have headaches, colds and other physical illnesses, as well as psychological problems to include social anxiety, depression, and suicidal ideation (Wolpert, 2008)(Billitteri, 2008). Cyberbullying has been defined in the 2011 publication from the White House Conference on Bullying Prevention as "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices" (Hinduja and Patchin, 2011). Just a few short years ago, it would have been impossible to victimize on such a grand and far-reaching scale. Now using one of the myriad forms of social media technology,

this form of bullying is convenient, impersonal and less risky for the bully than traditional schoolyard bullying. Since the majority of police agencies still lack personnel assigned to investigate social media or cybercrimes, the potential for these crimes to go undetected is great (Bockrath, 2010).

Unfortunately, cyberbullying itself has evolved into a hybrid form of traditional bullying and cyberbullying. School officials, counselors, and police officers assigned to schools have testified to the rampant practice of youth using social media to solicit another youth to "beat up" someone for them. This practice involves someone posting or tweeting a request for a volunteer to agree to assault another youth in return for money, another commodity or for the thrill. Once the agreement is reached, the perpetrator will often approach the unsuspecting victim and "punch them" or assault them without saying a word or explaining the motive. The victim is often left completely perplexed by the seemingly random assault, until further investigation by school officials or police reveal the convoluted motive. In one instance, it was not until several of these incidents were solved that school officials and police discovered why the random crimes were occurring. An extension of more traditional cyberbullying (whereby the perpetrator attacks the victim virtually online), this hybrid model allows the bully to hide behind a cloak of anonymity while reaching out and hurting their victim. This allows the initiating bully to remain anonymous to his or her victim while "contracting out" the physical portion of bullying, thus shielding the initiator from the psychological effects of having to witness the victim's experience of pain and suffering. In many ways, the initiator can treat this interaction as if he or she were simply playing a video game.

Through the collaborative and coordinated efforts of law enforcement, lawmakers, schools, parents and the community we can begin to effectively address the challenges associated with the various forms of social media related crime and victimization. These efforts can best be synchronized using a three-pronged approach to include:

- Collaboration and Partnerships
- Education
- Legislation

This three-pronged approach provides the framework for a comprehensive, multi-disciplined approach to address emerging issues associated with social media. Each approach will provide a better definition of the issues and offer common sense approaches to addressing the challenges.

Collaboration and Partnerships

The first approach involves collaboration and partnerships amongst law enforcement agencies to enhance their expertise in computer crimes that involve the social realm. This approach highlights the importance of law enforcement and other government agencies working together to share time, resources, training, expertise and personnel to address social media related crime. The prohibitive cost of the computer hardware and software necessary for forensic computer investigations, and amount of time often required to methodically investigate, search for, and process digital evidence can be more than most mid-sized law enforcement agencies can manage with limited resources.

Perhaps the best way to address the logistics of this approach would be to create a joint Computer Forensic Unit and Digital Crime Scene Investigation Unit with sponsorship by several regional agencies, and be comprised of both sworn and non-sworn personnel. This collaboration allows costs to be shared equitably, and also to enable the participating agencies to capitalize on the expertise and knowledge of other agencies to investigate cases. One of the most prominent examples of this collaboration is the newly formed Orange County Regional Computer Forensics Laboratory (OCRCFL) located in Santa Ana, California. The laboratory is funded by the Federal Bureau of Investigation (FBI) and is made up of ten participating agencies that assist with Regional, State, and Federal cases. Often Federal or Regional taskforce, regionalization, or technology grants may be available to assist in funding these collaborative efforts (The Sheriff's Blogger, 2011). These new forensic units can also collaborate with existing Federal, State or Regional taskforces to address complex, multi-jurisdictional, or interstate investigations beyond the authority or capability of the local law enforcement. Partnerships may also include the non-profit and private sector for training, research and funding opportunities through such organizations as SEARCH.org or Guidance Software.

Education

Education includes internal and external awareness of social media related crime and victimization. The first step is to educate public safety agencies and develop a comprehensive understanding and impact of social media related crimes. Strategies should also be developed to determine what is needed from these agencies to assist in the identification, investigation and prosecution of these crimes. All sworn personnel and all

non-sworn field personnel should receive training on the recognition and investigation of these crimes and the proper procedure for the collection and retention of digital evidence associated with various social media technology platforms.

A second priority in education is to partner with school officials and advocacy groups to provide education of social media related crime and victimization. In addition, training to students, parents, teachers, administrators and school staff should be implemented. This would include preventing on-line cyberbullying and victimization and how to report being victimized or the victimization of another. With approximately 40% - 49% of on-line youth reporting being the victim of cyberbullying, this approach may have a significant impact on youth violence and suicide (Billitteri, 2008). Issues such as electronic aggression, extortion, intimidation, defamation or slanderous postings or impersonation of another (e-impersonation), unauthorized posting of surreptitious video or images, sexting, solicitation for acts of violence and gang recruitment and activity should be a part of the training curriculum as well.

Legislation

The final approach involves legislation. Law enforcement, educators, parents and advocates must work with lawmakers to educate them about social media related crime and victimization, and the various laws or lack thereof in place to address them. Although recent legislation has been adopted to help close these loopholes, resistance from Internet providers, social media technology providers, and first amendment rights groups have prevented legislation that would better protect users and assist law enforcement in their efforts to identify, investigate, and prosecute social media related crimes.

Opposition to these legislative efforts often pits Internet providers and social media technology providers against the first amendment rights groups on some key issues. Law enforcement and legislators have at times found themselves siding with each of these groups on different issues. Internet providers and social media technology providers often seek to obtain as much user information and search history as possible in order to use or sell this information for marketing or the creation of user focused content or applications. In a 2009 New York Times article regarding the disclosed steroid use by baseball player Alex Rodriguez, Cindy Cohen, the legal director of the Electronic Frontier Foundation, calls this data collection "the surveillance business model." She states "…there is money to be made from knowing your customers well — with a depth unimaginable before Internet cookies allowed companies to track obsessively online behavior" (Cohen, 2009).

Internet providers and social media technology providers often retain this information for various time periods ranging from 30 days to several months or more. They are very hesitant, though, to admit they possess this information, and even more reluctant to surrender it when asked to do so or when served with a court order as a part of a criminal investigation. At times they may deny having possession of this information to avoid having to surrender it (Cohen, 2009). Meanwhile, first amendment rights groups oppose the collection of this information or any attempts to retain it or use it for marketing purposes without the user's consent. This opposition includes efforts to prevent law enforcement, other government agencies, and legislators from passing laws mandating the limited retention of any user information or history that could be used to identify the user and track their activity, even when such activity is criminal in nature.

Cohen states “The foundation argues that online service providers — social networks, search engines, blogs and the like — should voluntarily destroy what they collect, to avoid the kind of legal controversies the baseball players' union is now facing” (Cohen, 2009). Cohen’s comment was in reference to the fact the union did not destroy the 2003 urine sample before federal prosecutors seized it under court order. She later refers to the retention of on-line user data by saying, "You don't want to get a subpoena. For ordinary Web sites it is a cost to collect all this data" (Cohen, 2009). This position establishes a serious impediment to law enforcement efforts to protect the citizenry by obtaining the necessary evidence to enable them to identify, investigate and prosecute criminal acts perpetrated on-line. Fortunately, recent legislation is working to support and protect the user.

Beginning January 2011, California law prohibits the intentional on-line impersonation of another resulting in the harm, embarrassment or the endangerment of that person. This Senate Bill 1411 was introduced by Senator Joe Simitian (D-Palo Alto) (Simitian, 2010). This significant legislation builds on Assembly Bill 86, introduced by Assemblyman Ted Lieu (D-Torrance), adding cyberbullying to California Education Code 48900 (r) (Gjerde, 2009). This law enacted in January 2009, empowers California schools to suspend or expel students for acts of cyberbullying committed while on school grounds, during a lunch break off campus, or while traveling to or from school or a school sponsored event. The California Education code 48900 (r), however, does not address cyberbullying perpetrated against one student by another while not engaging in the activities enumerated in the code. UCLA Psychology Professor Jaana Juvonen states, “There is no reason why cyber-bullying should be ‘beyond’ the school’s responsibility to

address. Rather, it seams that schools need to enforce intolerance of any intimidation among students, regardless of whether it takes place on or beyond the school grounds" (Wolpert, 2008). It is presumed that any form of cyberbullying perpetrated against one student by another will affect the victimized student's ability to focus on and participate in their education or feel safe on campus (Stopbullying.gov) (Hinduja and Patchin, 2011). Studies have shown that victims of cyberbullying are more likely to get a detention or be suspended, to skip school, and experience emotional distress (Stopbullying.gov).

Perhaps the most effective way to protect students from cyberbullying would be to amend the California Education and Penal codes to mandate the reporting of these acts by school staff when the conduct is perpetrated by another student. The Legislature should also consider shielding the identity of the reporter to ensure they do not face the threat of civil recourse by parents, students or their lawyers for taking action or school sanction to stop the bullying behavior. Criminal statutes should also be enacted to prevent anyone from becoming the victim of intentional cyberbullying or any form of "electronic aggression". Efforts to address cyberbullying won another victory in October 2010, when Facebook vowed to begin aggressively trying to curb cyberbullying by using pop-up warnings and cancelling accounts of people who engage in this behavior (Chen, 2010).

Law enforcement, prosecutors and victims advocacy groups should lobby and educate lawmakers about the need of law enforcement investigators to obtain suspect user identification and activity from internet service and social media technology providers when served a court order. This would require the mandated retention of user identity and history for approximately 30 -90 days, and the surrendering of that information upon court order for the purposes of a criminal investigation. This would also include statutes

mandating Internet service providers, social media technology providers, and mobile media providers, to require users to provide their true name and address information when subscribing to services.

Conclusion

Social media technology has profoundly changed the way we communicate. This new revolution in communication has ushered in many new and exciting ways by which we can communicate, share and experience life, family, friendships, and the world around us with others. It shrinks the world into a much smaller and more personal global community that further illustrates that we all fundamentally desire the same things out of life and are much more alike than we are different. Although, this new communication revolution comes with increased risk of exposure, exploitation, vulnerability and risk of victimization, we can leverage or mitigate that risk through deliberate and thoughtful collaboration, education and appropriate legislation. When these three approaches are effectively leveraged to address these risks, this new communication revolution may be enjoyed by all with less thought given as to how it may be used to exploit us.

References

- Billitteri, Thomas. (2008). Cyberbullying. *CQ Researcher, 18*(17), 385-408. Retrieved March 7, 2010, from http://www.cqpress.com/product/Researcher-Cyberbullying-v18-17.html.

- Bockrath, P.J. (2010). Law Enforcement Cybercrime Unit Survey [Research Study]. *Surveymonkey.com*. Available from June 12, 2010 Web site: http://www.surveymonkey.com/MySurvey_EditorPage.aspx?sm=QGEAW1cjeBn3p5gtA39%2bQd3lh7Kk0yBwkKkooBSAeeQ%3d.
- Chen, Stephanie. (2010, October 5). In a wired world, children unable to escape cyberbullying. *CNN*. Retrieved April 7, 2010, from CNN Web site: http://edition.cnn.com/2010/LIVING/10/04/youth.cyberbullying.abuse/index.html?hpt=Sbin.
- Cohen, Noam. (2009, November). As data collecting grows, privacy erodes. *The New York Times*. Retrieved November 30, 2010, from The New York Times Web site: http://www.nytimes.com/2009/02/16/technology/16iht-16link.20207285.html.
- Facebook. (2010). *Facebook Press Room*. Retrieved May 16, 2010, from Facebook Web site: http://www.facebook.com/press.php.
- Gjerde, Jon. (2009, January 16). Cyber-bullying law gives schools more authority. *The California Aggie*. Retrieved January 10, 2011, from The California Aggie Web site: http://theaggie.org/article/2009/01/16/cyberbullying-law-gives-schools-more-authority.
- Hinduja, S. and Patchin, J.W. (2011). *Overview of cyberbullying*. White House Conference on Bullying Prevention. Retrieved March 25, 2011, from Stopbullying.gov Web site: http://www.stopbullying.gov/references/white_house_conference/white_house_conference_materials.pdf#overview_of_cyberbullying

- Lenhart, Amanda., & Madden, Mary. (January 7, 2007). Social Networking Websites and Teens. In Pew Internet (Ed.), *Pew Internet & American Life Project* (Teens, Social Networking). Retrieved May 17, 2010, from Pew Internet Web site: http://www.pewinternet.org/Reports/2007/Social-Networking-Websites-and-Teens.aspx.
- Simitian, Joe: California State Senator for the 11th District. (2010). SB 1411: Criminal E-personation (2010). Retrieved January 10, 2011, from State Senator Joe Simitian Web site: http://www.senatorsimitian.com/entry/sb_1411_criminal_e_personation/.
- The Sheriff's Blogger: Crime and punishment in and around Orange County, California. (2011, January 6). Law Enforcement Agencies Launch Orange County Regional Computer Forensics Laboratory to Fight High-Tech Criminals and Solve Cyber Crimes. [Web log story]. Retrieved from http://capistranoinsider.typepad.com/the_sheriffs_blogger/2011/01/law-enforcement-agencies-launch-orange-county-regional-computer-forensics-laboratory-to-fight-high-t.html. (2011, April 7).
- Wolpert, Stuart. (2008, October 2). Bullying of teenagers online is common, UCLA psychologists report. *UCLA Newsroom*. Retrieved April 8, 2011, from UCLA Newsroom Web site: http://newsroom.ucla.edu/portal/ucla/bullying-of-teenagers-online-is-64265.aspx.